Datenschutz-Zertifikat – nur sicher mit dem Siegel?

mit ISO 27701 . Dr.tech Wolfgang Prentner . IT-Ziviltechniker . Informatiker . Gerichtssachverständiger

Do. 25.2.2021. Webinar . Online Präsentation

V1.0, 26.02.2021 Wien

ZTP
IT-PRÜFSTELLE

CYBERBELT©

IHR INTERNET-SICHERHEITSGURT

cyberbelt.net

Sicherheits-Audit

Pentesting

Social Hacking

Red Team Operations

Code Analysen

mit **Zertifikat**

ZTP

Wir **übernehmen** die **Kontrolle**
Ihrer Unternehmensnetzwerke und Daten!

SOCIAL HACKING
Red Team Operations

ZTP
IT-PRÜFSTELLE

GUTACHTEN ZUR **DSGVO**

DATENSCHUTZ IM **UNTERNEHMEN**

mit Zertifikat . staatlich befugt und beeidet

- Erst-Inspektion mit Quick-Assessment
- Ergebnisse binnen 14 Tagen

Für mehr **Sicherheit**, **Vertrauen** und **Transparenz** in der **Informationstechnologie**

ZTP
IT-PRÜFSTELLE

Inhalt

- Rückblick Webinare DSGVO 2018
- Der IT-Ziviltechniker

- Datenschutzgrundverordnung
- Das Dilemma mit der DSGVO
- Datenschutz-Prüfung
- Datenschutz-Gutachten
- Datenschutz-Zertifikat
- Zusammenfassung

Video >>

IT-Ziviltechniker
mit staatlicher Befugnis

HERAUSFORDERUNGEN

- Ordentl. Kaufmann
- Techn. Gesetze
- Techn. Governance
- Techn. Compliance
- Techn. Standards

PROBLEME

- Cybercrime
- IT-Mitarbeiter
- IT-Dienstleister

Admin (!)

DAS PLUS

- Haftung
- ... mit Brief und Siegel
- Zertifikat

IT-Prüf- und Überwachungsstelle

Systeme . Software . Projekte . Datenschutz . IT-Kosten

ZTP IT-PRÜFSTELLE

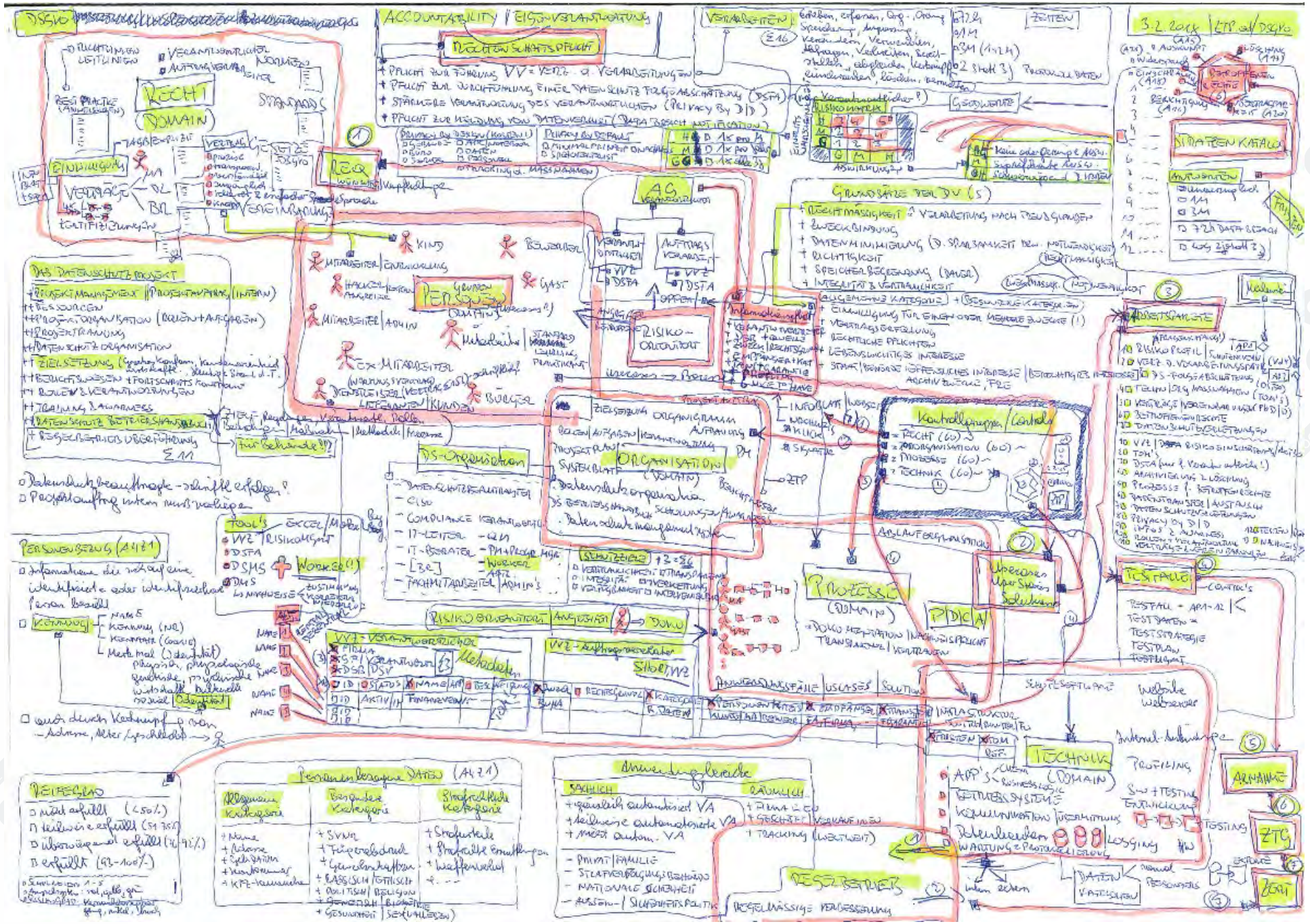
Datenschutz-Grundverordnung DSGVO

DSGVO Strafen

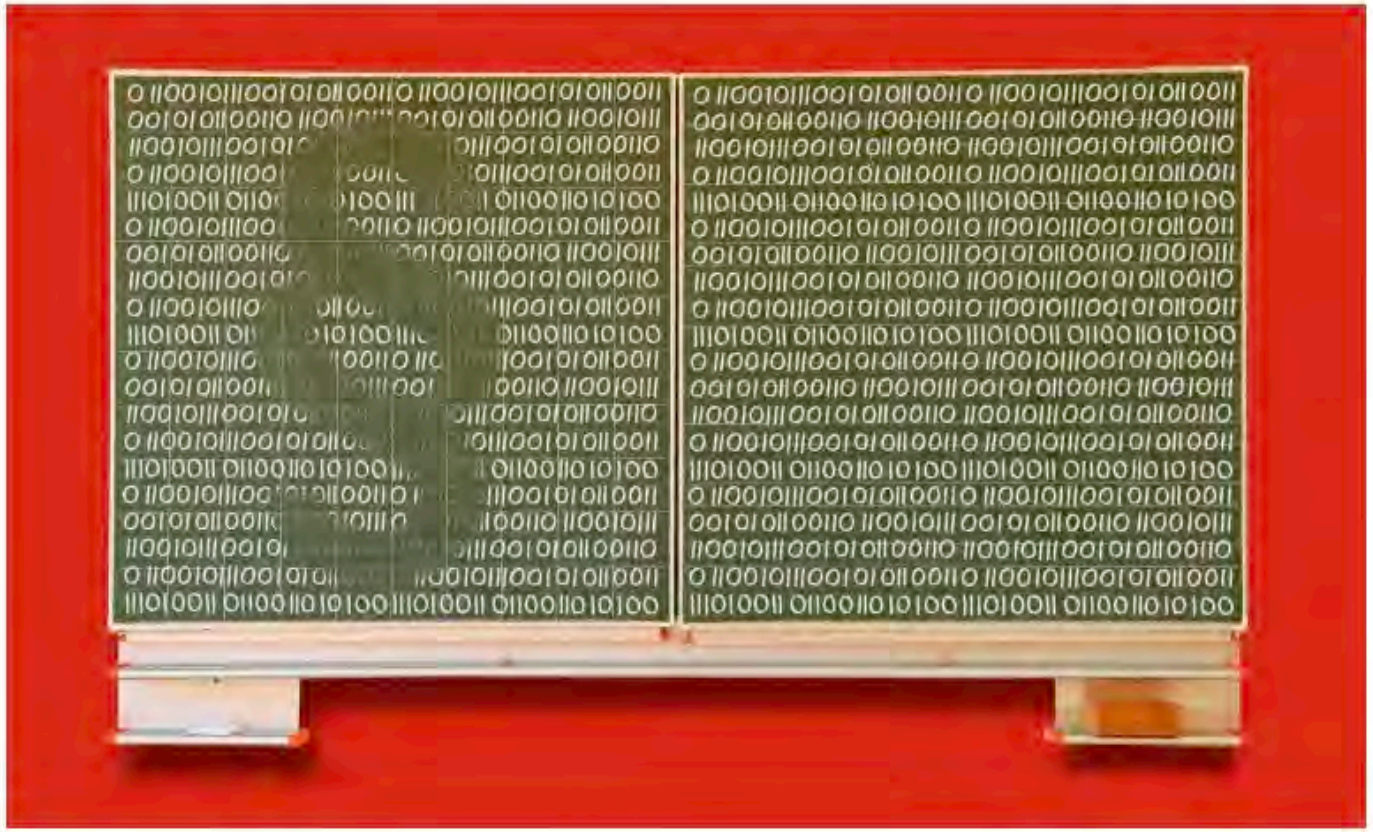
- 204 Mio. Euro gegen British Airways (England)
- 110 Mio. Euro gegen Marriott (England)
- 50 Mio. Euro gegen Google (Frankreich)

- 18 Mio. Euro gegen die **POST** (AT, Oktober 2019, aufgehoben wegen Formalfehler juristische versus **natürliche Person**)

- Urteil Schrems 2 – Achtung Office 365/Cloud



Das Dilemma mit der DSGVO



Wo versteckte personenbezogene Daten lauern

Böse Überraschung

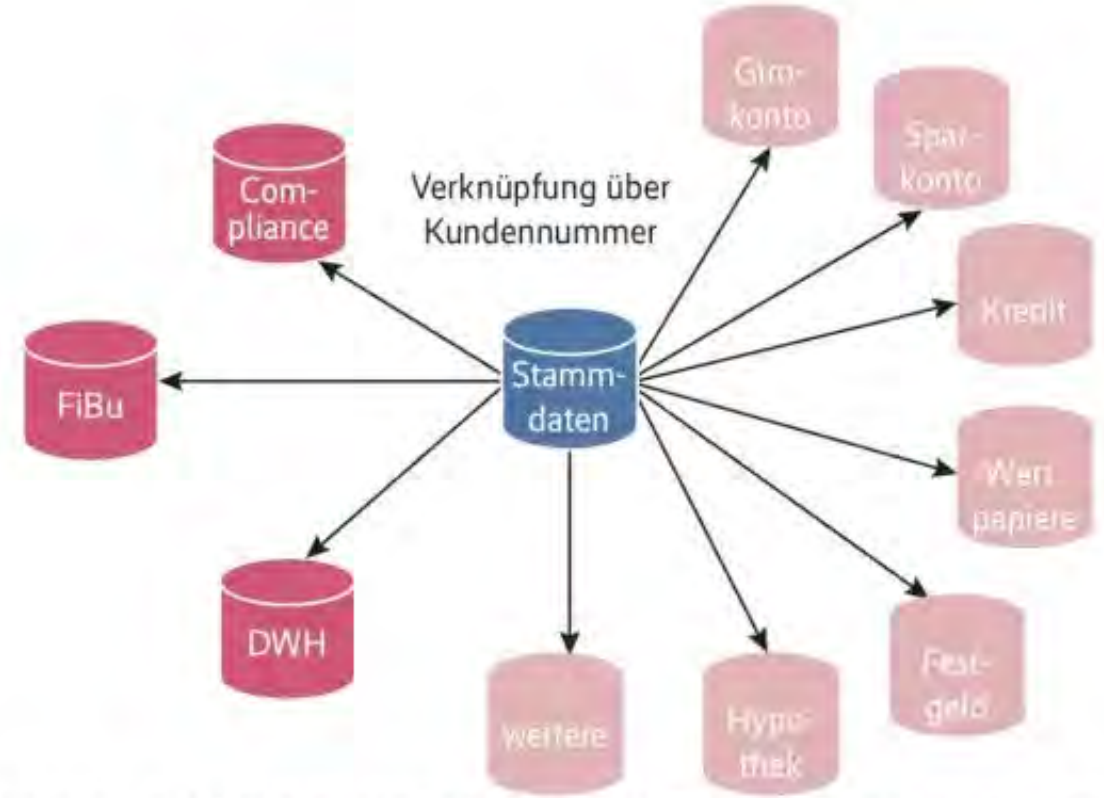
Martin Gerhard Loschwitz

Durch die Löschpflicht der DSGVO können vergessene Datensenken im Unternehmen zu einem echten Problem und verdammt teuer werden. Wo liegen heikle Daten, wie stöbert man sie auf und wie verhält es sich mit WORM-Archiven? iX hilft bei der Spurensuche.

Akribische Untersuchungen sind notwendig

TITEL | LÖSCHEN NACH DSGVO

iX 11/2020 S. 64



So etwa sieht die Systemlandschaft in einer Bank aus. Jedes Datenhaltungssystem speichert nur Teile eines kompletten Datensatzes. Löschen ist hier kompliziert (Abb. 1).

Löschkonzepte gemäß DIN 66398

Die Leitlinie DIN 66398 enthält Hilfestellungen für die kniffligen Fragen, die sich Unternehmen im Zusammenhang mit DSGVO-konformem Datenlöschen stellen.

Quelle: Deutsches Institut für Normung

Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig

Was die Datenschutzbehörden Anfang Oktober veröffentlicht haben, bewegt sich irgendwo zwischen unverschämt und weltfremd, findet Heise-Justiziar Joerg Heidrich.

Lesezeit: 4 Min. In Pocket speichern 24

(Bild: dennizn/Shutterstock.com)

23.10.2020 06:00 Uhr | c't Magazin

Von Joerg Heidrich

ISO 27701 - DSGVO konform?

APA OTS

SECURITY CIS CERTIFICATION INFORMATION

Erstes Datenschutz-Zertifikat mit internationaler Geltung: ISO 27701 kommt nach Österreich

CIS wurde als erste nationale Prüfstelle akkreditiert – Haftungsminimierung durch Sorgfaltsprinzip.

Wien (OTS) - Während die EU beim Thema Datenschutz hohe Strafen vorsieht, ist eine anerkannte Datenschutz-Zertifizierung bis heute ausständig. Besonders prekär ist dies, weil ein Daten-Eigentümer mithaftet, wenn bei seinem Provider eine Datenpanne passiert und er sich keinen Nachweis für sorgfältiges Vorgehen eingeholt hat. Ohne Zertifizierung war dies bis dato aber schwierig.

JA

ISO 27701 – Endlich eine DSGVO-konforme Datenschutz-Zertifizierung?

27 September, 2019

pwc | Deutschland

Die Artikel 42 und 43 der DSGVO regeln, unter welchen Voraussetzungen Zertifizierungen im Datenschutz zulässig sind und welche Anforderungen die Zertifizierungsstellen erfüllen müssen.

Bei näherer Betrachtung des Artikel 43 ist sofort ersichtlich, dass Datenschutz-Zertifizierungen nur auf Grundlage der ISO 17065 (Zertifizierung von Produkten und Prozessen) möglich sind. Dies bekräftigte das European Data Protection Board in seinen Guidelines zu diesem Thema (Guidelines 1/2018 und Guidelines 4/2018). Zertifizierungen von Datenschutz-Management-Systemen sind somit ausgeschlossen.

Des Weiteren haben ISO-Normen eine entscheidende Schwachstelle, was die Transparenz des Gültigkeitsbereichs beziehungsweise der angelegten Kriterien anbelangt. Oftmals kann anhand des Zertifikates nicht erkannt werden, welche Bereiche tatsächlich zertifiziert wurden. Dies widerspricht den Anforderungen an Datenschutz-Zertifizierungen, die Artikel 42 DSGVO vorgibt.

Fazit: Eine Zertifizierung nach der ISO 27001/27002 in Verbindung mit der ISO 27701 ist nicht DSGVO-konform.

Nein

ZTP

Datenschutz . Informationssicherheit . IT-Sicherheit

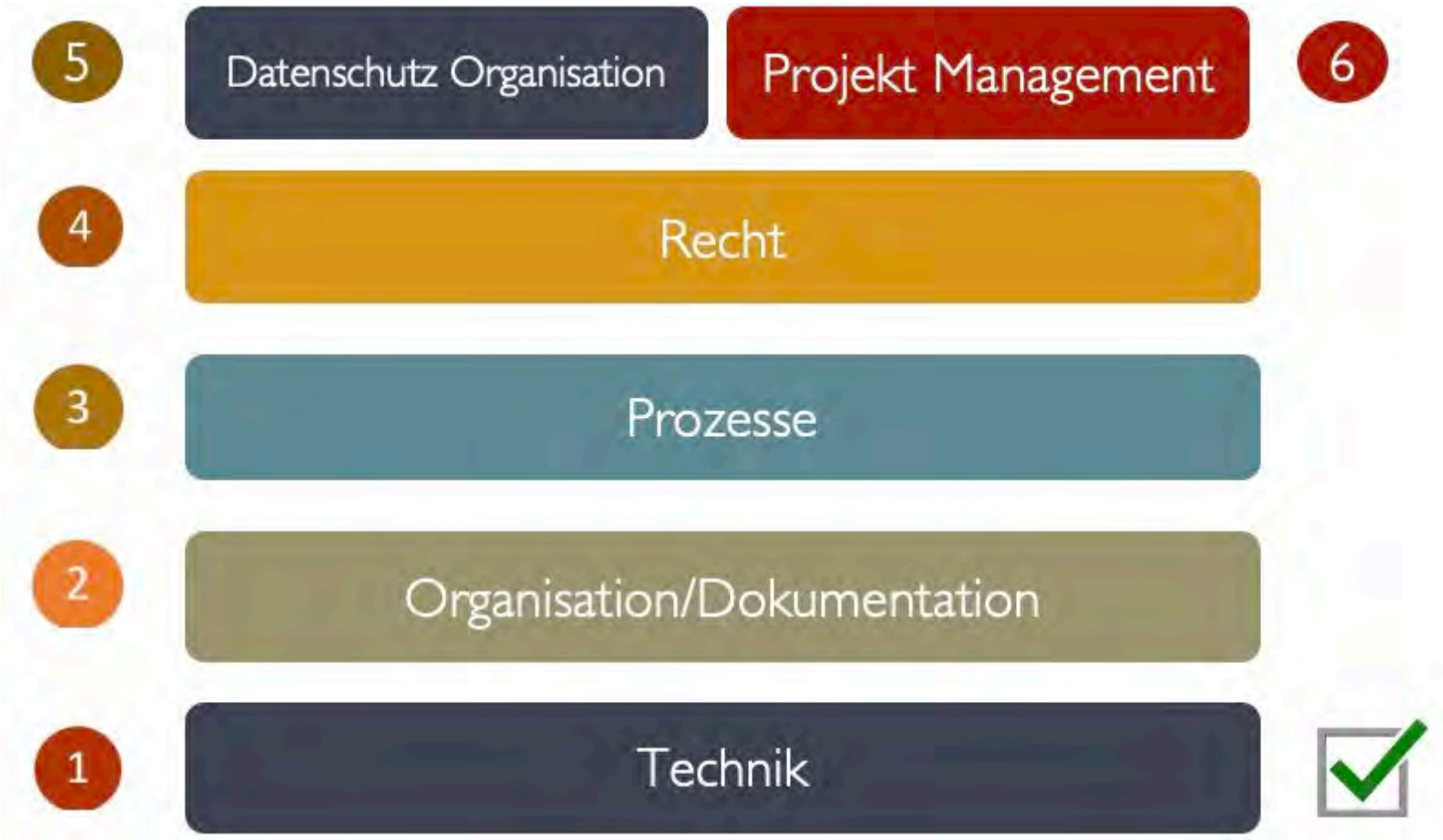
Organisatorischer **Datenschutz**
Management System

Technischer **Datenschutz**
Management System

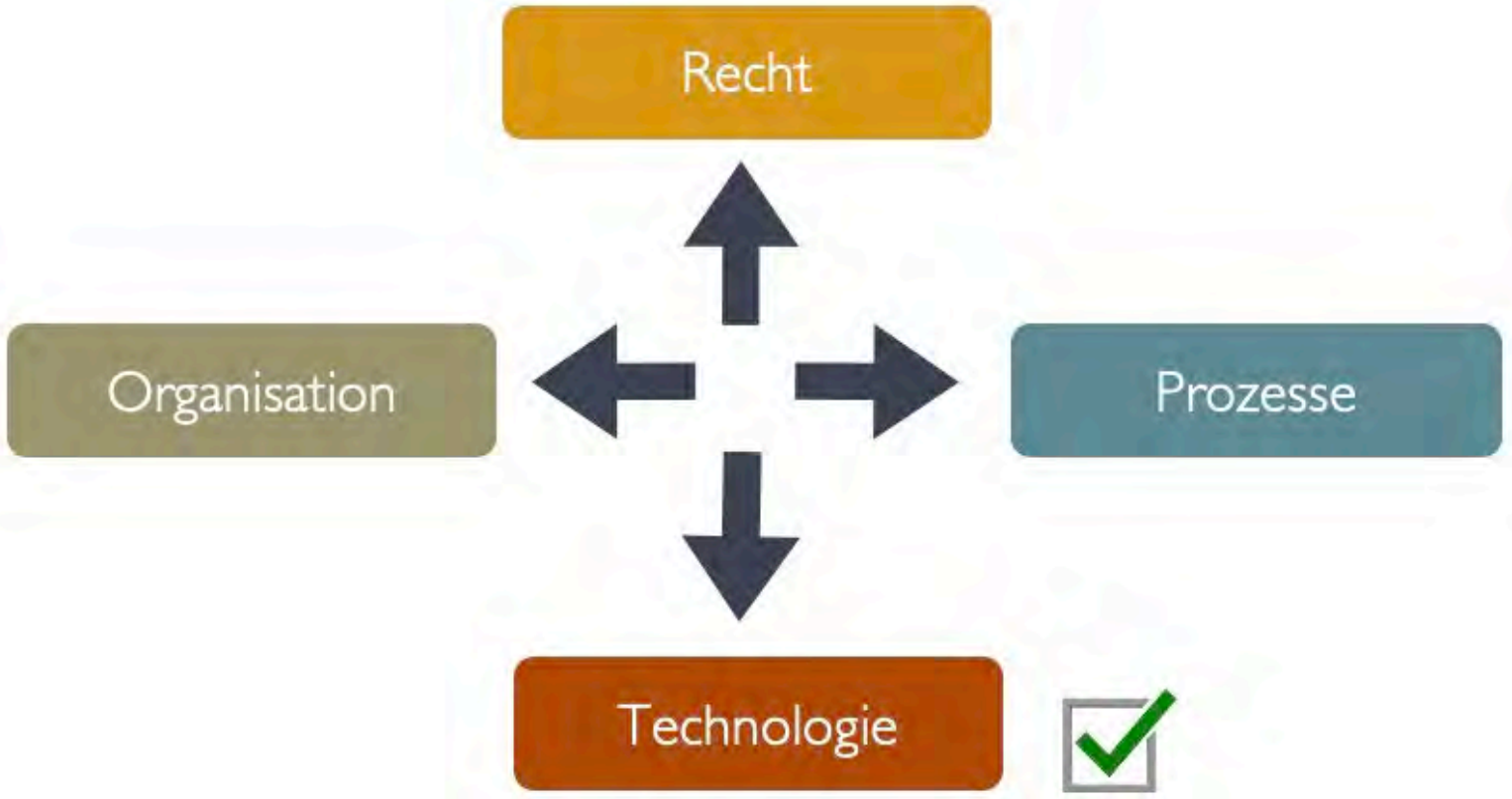
Technische **System-Sicherheit**
Software . Hardware . Systeme . Netzwerke .

3 Datenschutz-Prüfung

DSGVO-Architektur



Bereiche der DSGVO



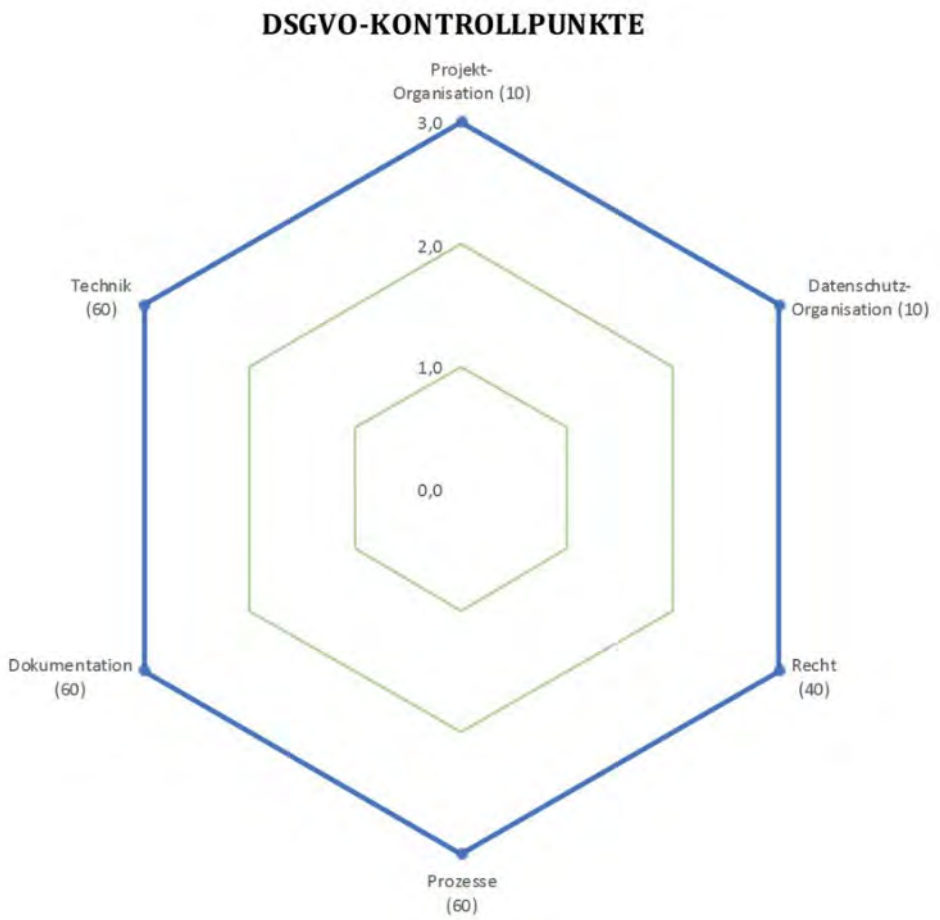
Kontrollpunkte zur DSGVO Zertifizierung

6 Bereiche mit KP - Kontrollpunkten

Projekt-Organisation (10)	KP 1: Projektauftrag vorhanden und unterfertigt?	3	2,8
	KP 2: Projektleiter und Mitarbeiter bestimmt?	3	
	KP 3: Projekt-Organigramm vorhanden?	3	
	KP 4: Projektplan vorhanden?	2	
	KP 5: Projekt-Controlling vorhanden?	3	
Datenschutz-Organisation (10)	KP 6: Datenschutzbeauftragter definiert?	3	2,6
	KP 7: Datenschutz-Organigramm vorhanden?	2	
	KP 8: Kontroll-Gremium vorhanden?	3	
	KP 9: Informationsfluss im Krisenfall definiert?	2	
	KP 10: Geschäftsführung – und Bereichsleitung involviert?	3	
Recht (40)	KP 11: Informationsverpflichtungen (12) auf Homepage, Verträge, Vereinbarungen erfüllt?	3	2,2
	KP 12: Einwilligung(en) notwendig?	2	
	KP 13: Grundsätze (5) der Verarbeitung von personenbezogenen Daten berücksichtigt?	1	
	KP 14: Betroffenenrechte (6) berücksichtigt?	2	
	KP 15: VVT als VA & AV aus rechtlicher Sicht freigegeben?	3	
Prozesse (60)	KP 16: Prozess: Auskunft (2) (Postiv- und Negativfall)?	3	2,7
	KP 17: Prozess: Widerspruch (2) (Postiv- und Negativfall)?	3	
	KP 18: Prozess: Einschränkung (2) (Postiv- und Negativfall)?	2	
	KP 19: Prozess: Berichtigung (2) (Postiv- und Negativfall)?	2	
	KP 20: Prozess: Übertragbarkeit (2)(Postiv- und Negativfall)?	3	
	KP 21: Prozess: Löschung (2) (Postiv- und Negativfall)?	3	
Dokumentation (60)	KP 22: Datenschutzhandbuch vorhanden?	3	2,6
	KP 23: Datenschutzbeauftragter – Rechte und Pflichten dokumentiert?	2	
	KP 24: Verzeichnis der Verarbeitungstätigkeiten vollständig (VVT VA/AV)?	3	
	KP 25: Prozesse ausreichend bewertet und dokumentiert?	2	
	KP 26: IKS durch Wirtschaftsprüfer/STB: bestätigt?	3	
	KP 27: Vorhandene Prüfberichte und Zertifizierungen (ISO 27001, IS0 20000, Cobit, SAE, ...)?	3	
	KP 28: Risikobetrachtung?	2	
	KP 29: Datenschutzfolgeabschätzung (DSVA)?	3	
Technik (60)	KP 30: Inventarisierung der IT-Systeme und Daten(banken) vorhanden?	3	2,6
	KP 31: Netzwerk-Architekturplan vorhanden?	2	
	KP 32: TOM's umgesetzt?	3	
	KP 33: Datenschutz durch Technik umgesetzt?	3	
	KP 34: Datenschutz durch Datenschutz-freundliche Voreinstellung umgesetzt?	2	

Beschreibung	Wert
nicht erfüllt (0-49%)	0
teilweise erfüllt (50-75%)	1
überwiegend erfüllt (76-92%)	2
vollständig erfüllt (93-100%)	3

Assessment


DSGVO-KONTROLLPUNKTE
Projekt-
Organisation (10)
3,0
2,0
1,0
0,0
Datenschutz-
Organisation (10)
Recht
(40)
Prozesse
(60)
Dokumentation
(60)
Technik
(60)

4 Datenschutz-Gutachten

Ziviltechnikergutachten

Gutachten und Befund, Version 1.0

GZ: A 100/18, Lfd.Nr.: 54

Datenschutz-Grundverordnung

Inhaltsverzeichnis

Datenschutz-Zertifikat

Gültig bis 01/2022

DATENSCHUTZ

EU-Datenschutz-Grundverordnung

für

MUSTER GMBH

Musterfirma Gesellschaft m.b.H.
0000 Musterstadt, Musterstraße 00, www.musterfirma.at

Prüfung der geeigneten technischen und organisatorischen
Maßnahmen gem. Art. 25 und Art. 32 der EU-Datenschutz-Grundverordnung (DSGVO)

Überwachungszeitraum
1. Februar 2021 bis 31. Jänner 2022
Bestätigt gemäß Ziviltechnikergesetz[1]

ZTP.digital . Prüfstelle für Digitale Sicherheit
CEO ZT DI Dr.techn Wolfgang Prentner, staatlich befugt und beeidet
ZTP.digital ZT-GmbH, Kärntner Platz 40/3/3 Wien . NÖ . VBG
T: +43 1 532 46 86 0 . www.ztp.digital . office@ztp.digital . ztp.digital

ZT DI Dr.techn. Wolfgang Prentner
staatlich befugt geprüft

Wien, 01. Februar 2021

DATENSCHUTZ ZTP GEPRÜFT

[1] Ziviltechnikergesetz 1993, §4 Abs.3,: Ziviltechniker sind mit öffentlichem Glauben versehene Personen gemäß §292 Zivilprozeßordnung, RGBl. Nr. 113/1895, in der jeweils geltenden Fassung. Die von ihnen im Rahmen ihrer Befugnis ausgestellten öffentlichen Urkunden werden von den Verwaltungsbehörden in derselben Weise angesehen, als wenn diese Urkunden von Behörden ausgefertigt wären. Unter Berücksichtigung von ÖNORM 7700, BSI Websicherheit, ISO 27001.

Zusammenfassung

GUTACHTEN ZUR DSGVO
DATENSCHUTZ IM UNTERNEHMEN

mit Zertifikat . staatlich befugt und beeidet

Unabhängig.

Planen.
Prüfen.

Nur sicher mit dem Siegel.
Ihre ZiviltechnikerInnen.

- Erst-Inspektion mit Quick-Assessment
- Ergebnisse binnen 14 Tagen

Für mehr **Sicherheit**, **Vertrauen** und
in der **Informationstechnologie**

ZTP
IT-PRÜFSTELLE

Besten Dank

für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?

ztp.digital

Gesundheit für Ihre IT.

ZTP.digital ZT-GmbH

Prüfstelle für
Digitale Sicherheit

T: +43 1 532 46 68 0

F: +43 1 532 46 68 - 20

✉ office@ztp.digital

💻 www.ztp.digital

Wien . Niederösterreich . Vorarlberg

Austria . Europe

ZTP
IT-PRÜFSTELLE

Nicht erlaubte Tätigkeiten

Keine kommerzielle Entwicklung von Software

Keine kommerzieller Verkauf von Hardware oder Software

Keine kommerzieller Betrieb eines Rechenzentrums

Kunden von ztp.digital

Kunden von ztp.digital